UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/929,121	08/15/2001	Toyoaki Kishimoto	212668US6	1335

22850   7590   10/09/2008
OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER
TESLOVICH, TAMARA

ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
10/09/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

	Application No.	**Applicant(s)**
	09/929,121	KISHIMOTO, TOYOAKI
Office Action Summary	**Examiner**	**Art Unit**	
	Tamara Teslovich	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

    A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>08 July 2008</u>.
2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1 and 3-18</u> is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) <u>1 and 3-18</u> is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☐ All b)☐ Some * c)☐ None of:
        1.☐ Certified copies of the priority documents have been received.
        2.☐ Certified copies of the priority documents have been received in Application No. _____.
        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.
4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.
5)☐ Notice of Informal Patent Application
6)☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on July 8, 2008 has been entered.

Claim 2 remains cancelled.

Claims 1, 3-6, 9 and 13 are amended.

Claims 14-18 are newly added.

Claims 1 and 3-18 are pending and herein considered.

Response to Arguments

Applicant's arguments filed July 8, 2008 have been fully considered but they are not persuasive.

Applicant's first set of arguments appearing on pages 9-10 fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. Applicant claims that "Dwek, the applied primary reference, fails to teach or suggest the interaction between an

authentication server and a content providing server, as recited in independent claims 1, 9 and 13" but fails to specifically point out which "interactions" Dwek fails to teach. There exist within each of claims 1, 2, and 13 a number of different interactions between the authentication server and the content providing server, any of which could correspond to Applicant's "the interaction between an authentication server and a content providing server" as stated in his arguments. Instead, the majority of Applicant's arguments appearing on pages 9-11 of his response amount to general descriptions of the applied reference and general descriptions of the invention, without specifically pointing out which limitations within Applicant's claims the reference allegedly fails to teach.

In response to Applicant's next set of arguments appearing on page 12 regarding Dwek's alleged failure to teach or suggest "*that his system includes an authentication server that 'sends a notification to said content providing server by which said requested site is produced, that starting of service provision for said mobile information terminal is permitted, if the unique identification information is found registered with said customer database' as recited in independent claims 1, 9, and 13*" the Examiner respectfully disagrees. The Examiner would first like to draw attention to column 4, lines 31-43 wherein Dwek discloses registration of users of an online music delivery system in order that they may download an installation file for installing a copy of the music player 120 onto the user's computer system. The client interface server 112 ointerfaces with the music player 120 for allowing the user to browse or search the online music database 114 and to implement various features of an online music delivery system as is

described in more detail throughout the reference. This registration serves to place

unique identification information within a customer database, information that may be

used to tailor content, advertisements, and even players "skins." Within lines 26-30 of

column 4, Dwek discloses the use of a plurality of song file servers, all of which hold

content that the user may be interested in, and all of which may be searched by the

user through the client interface server holding the customer database with customer

information therein. Once a selection is made by the user, it is the client interface

server that may then send a notification to the particular song file server where the

desired information rests, so that the requested media may then be streamed to the

requesting user. In order for the system to know where to stream said media, an

internet connection between the user's music player and the online music library will

have been established through which the music player may be recognized (col.5 lines

9-24). Without the registration of the user, and the collection of unique identification

information related thereto, the user would be unable to create his "shared playlists"

stored at the server and available to other users and his own "personal channels"

(columns 9-10). The user would also be unable to receive musical selections matching

certain set target criteria related to their listening, as well as targeted advertisements.

Furthermore, this process of registering a user is not only inherent but also necessary

for Dwek's "pay-per-listen" button. In column 12, lines 16-22, Dwek teaches the use of

a pay per listen button in order to allow users to specifically order special pay-per-listen

events such as new releases and concerts. The users may be able to purchase real-

time content or content related to upcoming events. In column 15 lines 35-41, Dwek

provides additional insight into purchases that might be made through his system, including but not limited to CDs or downloadable music. There is no doubt that Dwek includes within his system the registering of users and collection of unique identification information related to their viewing habits and financial links allowing for them to request media in a variety of forms, a request which upon authentication provides users access to their requested online media. As such, the Examiner maintains that Dwek teaches sending notification to said content providing server by which said requested site is produced, that starting of service provision for said mobile information terminal is permitted, if the unique identification information is found registered with said customer database as claimed in claims 1, 9, and 13.

It is for those reasons stated above in view of the references in their entirety that the Examiner maintains her 35 USC 103(a) rejections of claims 1 and 3-13 as previously set forth, and repeated below in a form to reflect Applicant's amendments.

In response to Applicant's remarks concerning newly added claims 14-18, the Examiner respectfully maintains her rejection of claim 13. Furthermore, the Examiner has rejected newly added claims 14-18 under 35 USC 103(a) as unpatentable over United States Patent No. 6,248,946 to Norman Dwek and further in view of US Patent Application Publication 2002/0032027 A1 to Kirani.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 and 3-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over United States Patent No. 6,248,946 to Norman Dwek and further in view of US Patent Application Publication 2002/0032027 A1 to Kirani .

Regarding *Claim 1*, Dwek teaches a user authentication method for an authentication server which executes user authentication between a information terminal and a content providing server interconnected by an open network, comprising the steps of:

registering, at an authentication server, unique identification information with a customer database of said authentication server in advance, wherein said unique identification information is stored in said information terminal (col.4 lines 31-43);

presenting, from the authentication server, to said mobile information terminal, a recommended menu including a plurality of official site access information for accessing predetermined content providing servers, respectively (col.4 lines 26-30 and 43-67; col.10 lines 4-24)

receiving, at the authentication server, from said information terminal, the unique identification information and a request for registering one of said official site access information for accessing said content providing server with a personal menu via the open network (col.9 lines 31-45; col.10 lines 21-47 and 60-67);

determining, at the authentication server, whether said unique identification information received from said information terminal is registered with said customer database (col.12 lines 15-21; col.15 lines 34-40);

sending a notification from the authentication server to said content providing server by which said requested site is produced, that starting of service provision for said information terminal be permitted, if the unique identification information is found registered with said customer database (col.12 lines 15-21; col.15 lines 34-40);

registering, at the authentication server, said requested official site access information with said personal menu after receiving an acknowledgement response of said notification from said content providing server (col.10 lines 13-67); and

notifying, to said information terminal from said authentication server, a completion of said registration (col.10 lines 35-51).

Dwek fails to teach the abovementioned system wherein the information terminal is a "mobile information terminal."

Kirani teaches a media spooler system and methodology providing efficient transmission of media content between wireless devices and other wireless devices or servers (Abstract). Kirani's system includes a plurality of wireless devices attempting to communicate with target hosts or servers and a media spooler/gateway acting as a gateway between the devices and the servers. Each of Kirani's wireless devices includes its own identification code (par 95), including but not limited to an international mobile equipment ID assigned by and specific to the phone manufacturer (Table 5).

It would have been obvious to a person of average skill in the area at the time of

the invention to include within Dwek the wireless capabilities as described in Kirani in

order to provide for users connected to the Internet and other media and document

servers via mobile information terminals such as cellular phones and other handheld

devices in a secure manner.

Regarding **Claim 3**, the combined method of Dwek and Kirani teaches the user

authentication method according to Claim 1, wherein,

when registering said site access information, user authentication is performed

on the basis of said unique identification information and said mobile information

terminal requested to make display for prompting said user to enter a password of the

user (Karani pars 211, 229).

Regarding **Claim 4**, the combined method of Dwek and Kirani teaches the user

authentication method according to Claim 3, wherein,

in the registering, a charging server is instructed to charge said user for the use

of a service provided by said content providing server associated with said site access

information at the time of registering said site access information (Dwek col.12 lines 15-

21; col.15 lines 35-40).

Regarding *Claim 5*, the combined method of Dwek and Kirani teaches the user authentication method according to Claim 4, wherein,

in the registering, confirming, before instructing said charging server for the charging, that said user is a registered user of said charging server is included (Dwek col.12 lines 15-21; col.15 lines 35-40).

Regarding *Claim 6*, the combined method of Dwek and Kirani teaches the user authentication method according to claim 1, wherein said open network is the Internet, through which the unique identification information is transmitted as encrypted by a predetermined encryption algorithm by a Web browser installed on said mobile information terminal (Dwek col.5 lines 31-43; Kirani par 222).

Regarding *Claim 7*, the combined method of Dwek and Kirani teaches the user authentication method according to Claim 6, wherein the unique identification information is read, by said Web browser, from a flash memory (see Kirani pars. 7, 81, 89, 94-96, 134) installed on said mobile information terminal and the retrieved unique identification information is transmitted as encrypted by the predetermined encryption algorithm by said Web browser (Dwek col.5 lines 31-43; Kirani par 222).

Regarding **Claim 8**, the combined method of Dwek and Kirani teaches the user authentication method according to Claim 7, wherein said predetermined encryption algorithm is SSL (Secure Socket Layer) (Kirani par 222).

Regarding **Claim 9**, Levergood et al. teaches a user authentication server which executes user authentication between a information terminal and a content providing server interconnected by an open network, comprising

means for registering unique identification information corresponding to said information terminal (col.4 lines 31-43);

means for presenting, to said information terminal, a recommended menu including a plurality of official site access information for accessing predetermined content providing servers, respectively (col.4 lines 26-30 and 43-67; col.10 lines 4-24);

means for receiving, from said information terminal, the unique identification information and a request for registering one of said official site access information for accessing said content providing server with a personal menu via the open network (col.9 lines 31-45; col.10 lines 21-47 and 60-67);

means for determining whether the unique identification information received from said information terminal is registered with said customer database (col.12 lines 15-21; col.15 lines 34-40);

means for sending a notification to said content providing server, by which said requested site is produced, that starting of service provision for said information terminal

be permitted, if the unique identification information is found registered with said

customer database (col.12 lines 15-21; col.15 lines 34-40);

      means for registering the requested official site access information with said

personal menu after receiving an acknowledgement response of said notification from

said content providing server (col.10 lines 13-67); and

      means for presenting, to said information terminal, a completion of said

registration (col.10 lines 35-51).

      Dwek fails to teach the abovementioned system wherein the information terminal

is a "mobile information terminal."

      Kirani teaches a media spooler system and methodology providing efficient

transmission of media content between wireless devices and other wireless devices or

servers (Abstract). Kirani's system includes a plurality of wireless devices attempting to

communicate with target hosts or servers and a media spooler/gateway acting as a

gateway between the devices and the servers. Each of Kirani's wireless devices

includes its own identification code (par 95), including but not limited to an international

mobile equipment ID assigned by and specific to the phone manufacturer (Table 5).

      It would have been obvious to a person of average skill in the area at the time of

the invention to include within Dwek the wireless capabilities as described in Kirani in

order to provide for users connected to the Internet and other media and document

servers via mobile information terminals such as cellular phones and other handheld

devices in a secure manner.

Regarding **Claim 10**, the combined method of Dwek and Kirani teaches the user authentication server according to Claim 9, wherein said open network is the Internet, through which the unique identification information is transmitted as encrypted by the predetermined encryption algorithm by a Web browser installed on said mobile information terminal (Dwek col.5 lines 31-43; Kirani par 222).

Regarding **Claim 11**, the combined method of Dwek and Kirani teaches the user authentication server according to claim 10 wherein the unique identification information is read, by said Web browser, from a flash memory (see Kirani pars. 7, 81, 89, 94-96, 134) installed on said mobile information terminal and the retrieved unique identification information is transmitted as encrypted by the predetermined encryption algorithm by said Web browser (Dwek col.5 lines 31-43; Kirani par 222).

Regarding **Claim 12**, the combined method of Dwek and Kirani teaches the user authentication server according to claim 11 wherein said predetermined encryption algorithm is SSL (see Kirani par 222). .

Regarding **Claim 13**, Dwek teaches a user authentication server which executes user authentication between a information terminal and a content providing server interconnected by an open network, comprising:

a registering module configured to register unique identification information corresponding to said information terminal received from the information terminal with a customer database of said authentication server (col.4 lines 31-43);

an interface configured to present, to said information terminal, a recommended menu including a plurality of official site access information for accessing predetermined content providing servers, respectively (col.4 lines 26-30 and 43-67; col.10 lines 4-24);

an interface configured to receive, from said information terminal, the unique identification information and a request for registering one of said official site access information for accessing said content providing server with a personal menu via the open network (col.9 lines 31-45; col.10 lines 21-47 and 60-67);

a determination module configured to determine whether the unique identification information received from said information terminal is registered with said customer database (col.12 lines 15-21; col.15 lines 34-40);

an interface configured to transmit a notification to said content providing server, by which said requested site is produced, that starting of a service provision for said information terminal be permitted, if the unique information is found registered with said customer database by the determination module (col.12 lines 15-21; col.15 lines 34-40);

a registering module configured to register the requested official site access information with said personal menu after receiving an acknowledgement response of said notification from said content providing server (col.10 lines 13-67); and

an interface configured to present, to said information terminal, a completion of said registration (col.10 lines 35-51).

Dwek fails to teach the abovementioned system wherein the information terminal is a "mobile information terminal."

Kirani teaches a media spooler system and methodology providing efficient transmission of media content between wireless devices and other wireless devices or servers (Abstract). Kirani's system includes a plurality of wireless devices attempting to communicate with target hosts or servers and a media spooler/gateway acting as a gateway between the devices and the servers. Each of Kirani's wireless devices includes its own identification code (par 95), including but not limited to an international mobile equipment ID assigned by and specific to the phone manufacturer (Table 5).

It would have been obvious to a person of average skill in the area at the time of the invention to include within Dwek the wireless capabilities as described in Kirani in order to provide for users connected to the Internet and other media and document servers via mobile information terminals such as cellular phones and other handheld devices in a secure manner.

Regarding **claim 14**, the the combined method of Dwek and Kirani teaches the authentication server according to Claim 13, wherein the recommended menu including a plurality of official site access information includes a plurality of hierarchical levels of categories (Dwek col.10 lines 4-20).

Regarding **claim 15,** the combined method of Dwek and Kirani teaches the authentication server according to Claim 13, wherein the customer database is

configured to store a name, age, birthday, gender and address corresponding to a user

(Dwek col.10 lines 4-20, 52-59).

Regarding **claim 16**, the combined method of Dwek and Kirani teaches the

authentication server according to Claim 15, wherein the authentication server uses at

least one of the name, age, birthday, gender and address corresponding to a user to

generate the recommended menu (Dwek col.10 lines 4-20, 52-59).

Regarding **claim 17**, the combined method of Dwek and Kirani teaches the

authentication server according to claim 13, wherein the personal menu includes a

plurality of icons, each of which corresponds to a link to a website external to the

authentication server (Dwek col.9 lines 58-66; col.10 lines 35-47).

Regarding **claim 18**, the combined method of Dwek and Kirani teaches the

authentication server according to claim 13, wherein the authentication server and the

content providing server are remotely connected via the Internet (Dwek col.4 lines 53-

67).

Conclusion

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Tamara Teslovich whose telephone number is (571)

272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Tamara Teslovich/
Examiner, Art Unit 2137

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137